## REMARKS

Claim Changes

Claim 1 is amended to recite "encrypting said secure blocks using each of a plurality of keys for each of a plurality of classes of destination systems, each key being associated with a corresponding class of destinations systems, thereby forming a plurality of encrypted versions of secured blocks, such that each encrypted version of secured blocks is decryptable by only those destination systems that are in the corresponding class," and "grouping said unsecured blocks and the plurality of encrypted versions of secured blocks as the common data stream." Similarly, claims 12, 16, 24, 26, 27, and 28 are amended. These changes are based on page 9, para. [0029], lines 7-11, page 11, and para. [0032], lines 7-9 and para. [0033], lines 2-5 of the specification as filed. Thus, no new matter is added.

Claims 6 and 28 are amended to recite "[a] method, in a destination system... said method comprising: obtaining said common data stream, wherein said common data stream includes a plurality of encrypted versions of secure blocks and unsecure blocks of data, said encrypted versions of secure blocks being encrypted, using each of a plurality of keys, for each of a plurality of classes of destination systems, respectively; decrypting only a portion of said encrypted versions of secured blocks that is encrypted using at least one key associated with a class of the destination system, thereby forming decrypted secure blocks." These changes are based on page 11, para. [0033], lines 2-5 of the specification as filed. Thus, no new matter is added.

Claims 9 and 10 are amended to be consistent with claim 6 as amended.

Claim 13 is amended to be consistent with claim 12 as amended.

Claim 17 is amended to be consistent with claim 16 as amended.

Claim 29 has been newly added. Support for the new claim can be found on page 9, para. [0029], lines 3-4 of the specification as filed. Thus, no new matter is added.

Claim 30 has been newly added. Support for the new claim can be found on page 11, para. [0033], lines 2-5 of the specification as filed. Thus, no new matter is added

No amendment made is related to the statutory requirements of patentability unless expressly stated herein. No amendment is made for the purpose of narrowing the scope of any claim, unless Applicant had argued herein that such amendment is made to distinguish over a particular reference or combination of references. Any remarks made herein with respect to a given claim or amendment is intended only in the context of that specific claim or amendment, and should not be applied to other claims, amendments, or aspects of Applicant's invention.

Rejection of claims 1, 2, 4-9, 11-19, and 24-28 under 35 U.S.C. § 102 (a/e) as being anticipated by US 7,177,427 (Komuro)

Applicant respectfully traverses in part and amends in part. Applicant has amended the claims to clarify the invention. Applicant therefore respectfully requests reconsideration of the rejection of claims 1, 2, 4-9, 11-19, and 24-28 under 35 U.S.C. § 102(a/e) as being anticipated by Komuro.

Applicant respectfully submits that Komuro does not anticipate, either expressly or inherently, each and every element as set forth in independent claims 1, 6, 12, 16, 24, 26, 27, and 28. For example, independent claim 1 as amended, recites "encrypting said secure blocks using each of a plurality of keys for each of a plurality of classes of destination systems, each key being associated with a corresponding class of destinations systems, thereby forming a plurality of encrypted versions of secured blocks, such that each encrypted version of secured blocks is decryptable by only those destination systems that are in the corresponding class," which is not anticipated either expressly or inherently, in Komuro.

Komuro discloses a method for transferring information using an encryption mode indicator (EMI). Komuro discloses that a source device receives audio video information in the form of data packets. The received data packets include CCI (Copy Control Information), which is used for selecting either EMI mode A or EMI mode B. If EMI mode A is selected, the data packet is routed to encrypt unit A (418) and if EMI mode B is selected, then the data packet is routed to encrypt unit B (420). The result from either encrypt unit A (418) or encrypt unit B (420) is received by a multiplexer (422) and further forwarded to an interface (125) between the source device and a sink device. See col. 7, line 47 through col. 8, line 11 of Komuro. At the other end, the sink device receives the data packet and selects either decryption unit A (448) or decryption unit B (450) based on the EMI mode of the received data packet to decrypt the data packet. See col. 8, lines 17-50 of Komuro.

Komuro discloses that the data packet is encrypted either at encrypt unit A or encrypt unit B based on an EMI mode selected. The encrypted data packet is then sent by the source device to the sink device. At the other end, the sink device receives the data packet and based on the EMI mode of the sent data packet, the data packet is decrypted either at decryption unit A or decryption unit B. See col. 8, lines 35-50 of Komuro. However, Komuro's sink device simply decrypts all the received data packets irrespective of class of the sink device and does not decrypts only those packets that are encrypted using a key associated with a class of the sink device. In contrast, Applicant's claim 1, as amended, recites "encrypting said secure blocks using each of a plurality of keys for each of a plurality of classes of destination systems...thereby forming a plurality of encrypted versions of secured blocks, such that each encrypted version of secured blocks is decryptable by only those destination systems that are in the corresponding class."

Further, Komuro simply discloses that the data packet is encrypted by a key either at encrypt unit A or encrypt unit B based on the EMI mode selected for the data packet. However, Komuro makes no mention that the key is associated with a corresponding

class of sink device. In contrast, Applicant's amended claim recites "each key being associated with a corresponding class of destinations systems."

Additionally, Komuro discloses that the data packet is encrypted by encrypt unit A or encrypt unit B, based on the EMI mode selected by the EMI mode select circuit. The encrypted data packet is then forwarded to the sink device through the interface 125. See col. 7, lines 59-65 and col. 8, lines 2-8 of Komuro. Therefore, Komuro discloses that the source device forms a single encrypted data packet to be sent to all sink devices, and does not forms a plurality of encrypted versions of data packets as required by the Applicant's claim. In contrast, Applicant's claim 1, as amended, recites "thereby forming a plurality of encrypted versions of secured blocks."

Further, Komuro discloses that, if EMI mode A is selected, then key A is used to encrypt the data packet and, if EMI mode B is selected, then key B is used to encrypt the data packet. See col. 9, lines 42-43 and lines 52-53 of Komuro. However, Komuro discloses that the data packet is encrypted using either key A or key B and does not discloses that the data packet is encrypted using each of the key A and key B. In contrast, Applicant's claim 1, as amended, recites "encrypting said secure blocks using each of a plurality of keys for each of a plurality of classes of destination systems."

Also, from item 4, page 3, of the Office Action, it appears that the Office Action equates Komuro's function of multiplexer with Applicant's "grouping." This analogy is, however, a mischaracterization of Komuro. Komuro discloses that a multiplexer selects only one output among the outputs of encrypt units. However, the multiplexer does not group the outputs of the encrypt units, as required by the Applicant's claim. See col. 7, line 67 through col. 8, line 2 and col. 8, lines 8-11 of Komuro. In contrast, Applicant's claim 1 recites "grouping said unsecured blocks and the plurality of encrypted versions of secured blocks as the common data stream."

Regarding claim 6, Komuro discloses that the sink device receives the encrypted data packets from the source device and based on the EMI mode of the received data packets, the data packets are decrypted. See col. 8, lines 35-50 of Komuro. However, Komuro's sink device simply decrypts all the received data packets irrespective of class of the sink device and does not decrypts only those packets that are encrypted using a key associated with a class of the sink device. In contrast, Applicant's claim 6, as amended, recites "decrypting only a portion of said encrypted versions of secured blocks that is encrypted using at least one key associated with a class of the destination system."

Further, as mentioned above, Komuro's multiplexer simply selects only one output among the outputs of encrypt units and routes the output to a BSR media. However, the multiplexer does not group the outputs of the encrypt units, as required by the Applicant's claim. See col. 7, line 67 through col. 8, line 2 and col. 8, lines 8-11 of Komuro. In contrast, Applicant's claim 6 recites "grouping said unsecure blocks and said decrypted secure blocks as a useful stream for use by said destination system."

Regarding independent claims 12, 16, 24, 26, 27, and 28, Applicant respectfully submits that the above discussed argument apply equally to the limitations of claim 12, 16, 24, 26, 27, and 28. Applicant therefore respectfully requests withdrawal of the rejection of claim 12, 16, 24, 26, 27, and 28 under 35 U.S.C 102 (a/e).

Dependent claims 2-5, 7-11, 13-15, 17-19, 25 depend from, and include all the limitations of independent claims 1, 6, 12, 16, and 24, respectively. Therefore, Applicant respectfully requests the reconsideration of dependent claims 2-5, 7-11, 13-15, 17-19, 25 and requests withdrawal of the rejection.

Rejection of claims 3 and 10 under 35 U.S.C. § 103 (a) as being unpatentable over US 7,177,427 (Komuro) in view of US 5,864,747 (Clark)

Applicant respectfully submits that Komuro has been previously discussed and it has been clarified that Komuro fails to describe the above mentioned limitations of

independent claims 1 and 6. Applicant has carefully reviewed Clark and Applicant respectfully submits that Clark also fails to overcome the deficiency of Komuro in that Clark also does not describe the above mentioned limitations. Furthermore, claims 3 and 10 depend from, and include all the limitations of independent claims 1 and 6. Therefore, Applicant respectfully requests the reconsideration of dependent claims 3 and 10 and requests withdrawal of the rejection.

New Claims

Newly added dependent claim 29 depends from, and includes further limitations of the now believed allowable claim 1. Therefore, claim 29 is believed to also be allowable.

Newly added dependent claim 30 depends from, and includes further limitations of the now believed allowable claim 6. Therefore, claim 30 is believed to also be allowable.

Conclusion

Applicant respectfully requests that a timely Notice of Allowance be issued in this case. Such action is earnestly solicited by the Applicant. Should the Examiner have any questions, comments, or suggestions, the Examiner is invited to contact the Applicant's attorney or agent at the telephone number indicated below.

Please charge any fees that may be due to Deposit Account 502117, Motorola, Inc.

Dated: July 14, 2008

Respectfully submitted,

By: /Larry T. Cullen/

Larry T. Cullen
Registration No.: 44,489

Motorola Connected Home Solutions
101 Tournament Drive
Horsham, PA 19044
(215) 323-1907